ENVISTA FORENSICS

LARS DANIEL ENCE, CCO, CCPA, CTNS, CTA, CIPTS, CWA
PRACTICE LEADER - DIGITAL FORENSICS
JAKE GREEN CCO, CCPA, CASA, MCFE
SENIOR DIGITAL FORENSICS EXAMINER

CROSSING DIGITAL FORENSICS EXPERTS

ON COMPUTER AND CELL PHONE EVIDENCE

DIGITAL FORENSICS //

Class Outline

- General Recommendations
- Cross Examination Scripts From Actual Cases
  - Cell Phone Forensics
  - Computer Forensics
  - Google Location Services
  - Cellular Location
- Case Examples – Expert/Attorney Preparation
  - Aaron Hernandez
  - Casey Anthony
  - Capital Murder
  - Child Exploitation
- Problematic Expert Examples
  - Testimony Examples
- Ask Your Expert for Intel (even if you don't need them in your case)
  - Example Intel

ENVISTA FORENSICS

General Recommendations

- Ask for a list of prior testimony for the other side's expert.
  - Get transcripts
  - Look for changes in position or inconsistent answers in prior cases.
- Always ask if they have been prevented from giving expert testimony in any other case.
- Always ask if they have had their expert testimony limited in any way.
- Do a thorough Google search for publications, marketing, blog posts, etc.
- See if your Expert has prior knowledge of the other expert.
  - Does the expert have any transcripts of the other expert's testimony.
  - Have they to that experts training classes or read their publications?
- Are they an expert in EVERYTHING?
- Get their current CV AND the CV from when they did the examination.
- Ensure their qualifications are real (Forensic Certifications vs Certifications of Attendance)
- Use your expert as a source for developing cross exam questions.
  - Have your expert put in the expected correct answers for all technical questions so you can be sure you are getting accurate answers.

ENVISTA FORENSICS

CELL PHONE FORENSICS

CROSS EXAMINATION EXAMPLE

DIGITAL FORENSICS //

Cell Phone Forensics…"Expert"?

- Unqualified examiner
  - MD vs. Harry Jones
    - The examiner was not qualified to testify as an expert concerning cell phone forensics

Voir Dire – States Expert

Q: How many mobile devices have you examined?
A. ?

Q: When did you receive your Cellebrite certification?
A. “Should be on CV”

Q: How many times have you performed Cellebrite extractions for use in a criminal case?
A. ?

Q: How many times have you testified about the results of Cellebrite extractions in Court?
A. “Should be in testimony list.”

Q: What is the difference between and “extractions” and “analysis”?
A. An extraction is where the data is gathered or copied from a device. Analysis occurs after the extraction and is performed using a different tool set.

Q: How many devices have your analyzed?
A.?

Voir Dire – States Expert

Q: In the field of digital forensics, what does it mean to “validate” your findings?
A. Confirm or determine to be accurate

Q: In your training, specifically the Physical Analyst certification course, did Cellebrite instruct you to validate your evidence?
A. Yes

Q: What methods can be used to validate evidence?
A. Reviewing the raw data manually
Running the data with a second tool
Compare to another source like call detail records
Compare to another device extraction (other party in a conversation)
Manual Examination of the Device by powering it on and recording the screen

Q: You mentioned, SHA, what?
A. SHA256

Q: Does that validate evidence or verify an image?
A. That is an image verification, not validation

Voir Dire – States Expert

Q: What is the physical piece of hardware that Cellebrite sells?
A. Cellebrite UFED or Universal Forensic Extraction Device

Q: What is the name of the software that Cellebrite sells?
A. Physical Analyzer

Q: What are the default settings for UFED regarding the display of dates and times?
A. DAY MONTH YEAR and MILITARY TIME

Q: What are the default settings for Physical Analyzer regarding the display of dates and times?
A. MONTH DAY YEAR and Civilian Time with AM/PM

Voir Dire – States Expert

Q: Can you describe Cellebrite's three methods of extraction?
A. -Logical
-File System
-Physical

Q: What role does the Physical Analyzer software play in the extraction process?
A. Review of extractions, analysis of data, and production of reports

Q: Do you load your extractions into Physical Analyzer?
A. Yes

Q: Can you describe the three types of extractions?
A: Physical Extractions are the highest level; File System is intermediate; Logical is most basic

Q: Can you describe what the underlying data of a logical extraction looks like?
A. A series of HTML files which report how the UFED *reads* the phone's data

Q: Do you review the underlying data behind the extractions?
A. You should.

Voir Dire – States Expert

Q: Is it true that logical extractions do not export the SQLite “SEQUAL LIGHT” database in the which stores these messages?
A. Correct, the do not, they only read the database

Q: Can the database be extracted with a file system or physical extraction?
A. Yes

***Q: What is the technical term for a “text message”?
A. SMS

Q: What is an SMS?
A. Short Message Service

Q: What is the size of a single SMS message or text message?
A. 160 bytes

Q: What happens if SMS message exceeds the 160 character limit?
A. It is automatically converted into an MMS message.

Voir Dire – States Expert

Q: What are the common smart phone operating systems?
A. Android, Apple iOS, Windows Phones, Blackberry

Q: How does the Android operating system store text messages?
A. SQLite Databases

Q: What is the name of that database?
A. mmssms.db

Q: What time format is used to store dates and times in the mmssms.db?
A. UNIX Epoch time, or the number of seconds since January 1 1970

Q: Is the mmssms.db time stored as UTC or local time?
A. UTC

Q: Does Cellebrite teach certified examiners to validate findings or rely on reports or extractions that have not been analyzed?
A. Validate findings

Voir Dire – States Expert

Q: In the course of analysis in any mobile devices, do you validate your findings?
A. ?

Q: What methods do you use to validate?
A. ?

Direct Exam – Overview

Q: How do mobile devices running the Android operating system store SMS messages?
A. In SQLite Databases (pronounced SEQUEL LIGHT)

Q: What is the name of the database where SMS messages are stored?
A. mmssms.db

Q: Does this database record the times that messages are received?
A. Yes

Q: What is the time format that these dates and times are stored?
A. Unix Epoch time, or the number of seconds since January 1, 1970

Q: Is this time dependent on time zone?
A. No, it is stored in UTC

Q: What does the term “UTC”?
A. Coordinated Universal Time

Direct Exam – Overview

Q: Can you briefly describe what UTC time means?
A. Primary Time Standard for clocks and machines running across the world. Global companies serve customers across many time zones, regardless of location, 24 hours a day. UTC allows computers to capture and record data, regardless of time zone.

Q: On Page 1 of your report, what does “Original UTC Value” mean?
A. The times have not been changed to local time. Cellebrite can provide dates and times in local time, based on the time zone set by the operating system.

Q: Did you confirm the time zone for this device?
A. It is set to Eastern Time (Detroit)

Q: What is local time in this case?
A. Eastern Time

Q: When converting UTC time to Eastern Time, what is the difference?
A. UTC-4: Eastern Daylight Time (March through November), UTC-5: Eastern Standard Time

Direct Exam – Extractions and Report

Q: What tool did you utilize to extract data from these devices?
A. Cellebrite

Q: What extraction methods did you attempt on Monica's device?
A. Logical and Physical

Q: Was the Physical extraction successful?
A. No

Q: Did Cellebrite produce an error?
A. Yes

Q: What types of extractions did you utilize to examine and extract the data?
A. LG: Logical
Motorola: Logical

Q: Is it within Cellebrite best practices to complete all three extraction methods?
A. Yes

Direct Exam – Extractions and Report

Q: Why did you not gather a file system for either device?
A. ?

Q: You discussed your training and experience, does Cellebrite train an examiner to validate their findings?
A. Yes

Q: How can an examiner validate their findings?
A. Using other forensic tools, review of raw data, peer review

Q: Did you review the actual, SQLite "SMS" database in this case?
A. No, because it is not extracted with the Logical method

Q: Per page 81, row 199 of your report's SMS section, what time was that message received?
A. June 16, 2015 5:43:42 PM (UTC+0)

Q: In local time, here in Maryland, when was this message actually received?
A. 1:43:42 PM

Direct Exam – Extractions and Report

Q: How do you know this?
A. The device's time zone is set to Eastern Standard Time or UTC -5. In the month of June, you would subtract 4 hours to set the time zone to local.

Q: So the message is recorded in the MMSSMS.db at 1:43 PM?
A. Correct

Q: Why did you not set the time zone in your report?
A. ???

Q: What methods did you use to validate your findings?
A. None?

Q: You stated that you "wrote a report" did you write a report in this case? Or did you simply export an automated report from Cellebrite?
A. Simple export

Direct Exam – Extractions and Report

Q: On line 199, you mention a “time issue”.
A. Yes

Q: And this time issue, you noticed it upon the preparation of your second report, is that correct?
A. : Yes

Q: Isn’t the second report a simple reloading of the old phone data into a newer version of forensic software?
A. Yes

Q: Does the software report based upon the old settings, or new settings?
A. Old settings

Q: Did you apply for a new warrant for this new search?
A. No

ENVISTA FORENSICS

COMPUTER FORENSICS

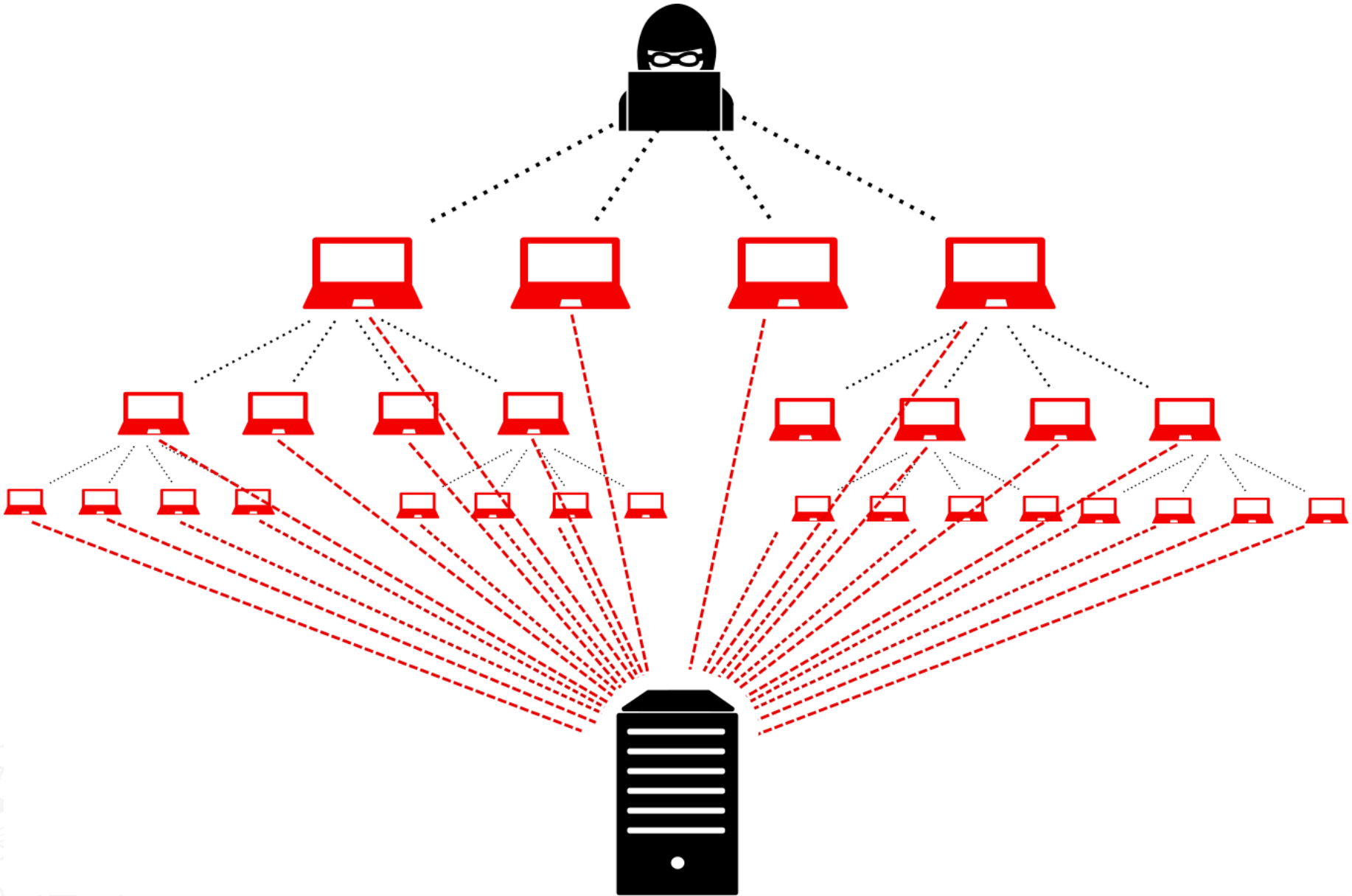
CROSS EXAMINATION EXAMPLE

DIGITAL FORENSICS //

Dark Web Cyber Attacks

- DDoS
  - Defendant was arrested and tried for operating a “booter service” which is a pay to DDOS (Distributed Denial of Service) website.
  - Defense theory – customers unable to cause actual damage using these services.
  - Impossible defense but defendant insisted on going to trial
- Objective
  - Preserve for Appeal
  - Sentencing Mitigation

DDoS



1 – Establish the fact that many issues could cause websites to be slow

Q. Can the time it takes to load an ecommerce web page be affected by things other than DDOS attacks?

A. Yes

Q. Would one of those things be a poorly designed web page?

A. Yes

Q. Could the customer's internet speed cause slow loading of web pages?

A. Yes

Q. Could the presence of malware programs on the customer's computer cause slow loading of web pages?

A. Yes

1 – Establish the fact that many issues could cause websites to be slow

Q. Could issues other than DDOS attacks at the customer's internet service provider cause slow loading of web pages?

A. Yes

Q. Could applications running on the customer's computer cause slow loading of web pages?

A. Yes

Q. Could congestion on the customer's home network problems for a customer, for example having the dreaded "buffering" of streaming services?

A. Yes

Q. So would it be fair to say that there are several reasons a person could have a bad experience that have nothing to do with attacks on web sites or network streaming services?

A. Yes

2 – Show the many options for DDoS without a booter service

Q. Earlier you explained that a DDOS attack is a Distributed Denial of Service attack, is that correct?

A. Yes

Q. Is it possible to launch a DDOS attack without the use of a booter service?

A. Yes

Q. Would using the LOIC (Low Orbit Ion Cannon) network testing tool be one way?

A. Yes

Q. Would the tool Slowloris be another way to launch a DDOS attack without a booter service?

A. Yes

Q. Tor's Hammer be another way to launch a DDOS attack without a booter service?

A. Yes

2 – Show that booter services are a tool – not only for malicious activity

Q. Does an account with a booter service mean that someone is planning to do an illegal attack on a server?

A. No

Q. In fact, didn't the FBI create an account on Downthem.org for the purpose of testing DDOS attacks?

A. Yes

Q. Isn't it true that the FBI created accounts on a number of booter services for the purpose of testing DDOS attacks?

A. Yes

Q. Have you ever, as part of your network security role, initiated a stress test DDOS attack against one or more of the servers under your control?

A. ???

3 – Show that booter services are a tool

Q. When someone creates an account with a booter service, do they have to agree to a "Terms of Service"?

A. Yes

Q. In fact, would a person who creates an account with Downthem.org required to agree to their Terms of Service?

A. Yes

Q. Would a person who creates an account with Ampnode.com be required to agree to their terms of service?

A. Yes

Q. Can you read for the court this excerpt from the terms of service for Ampnode.com?

3 – Show that booter services are a tool

A. "ALL SERVICES PROVIDED BY AMPNODE SERVERS MAY BE USED FOR LAWFUL PURPOSES ONLY. TRANSMISSION, STORAGE OR PRESENTATION OF ANY INFORMATION, DATA OR MATERIAL IN VIOLATION OF ANY UNITED STATES FEDERAL, STATE OR CITY LAW IS PROHIBITED. THIS INCLUDES, BUT IS NOT LIMITED TO: COPYRIGHTED MATERIAL, MATERIAL WE JUDGE TO BE THREATENING OR OBSCENE, OR MATERIAL PROTECTED BY TRADE SECRET AND OTHER STATUTE. THE "SUBSCRIBER", "CLIENT" AGREES TO INDEMNIFY AND HOLD HARMLESS AMPNODE HOSTING FROM ANY CLAIMS RESULTING FROM THE USE OF SERVICE WHICH DAMAGES THE "SUBSCRIBER", "CLIENT" OR ANY OTHER PARTY. PROHIBITED ARE SITES THAT PROMOTE ANY ILLEGAL ACTIVITY OR PRESENT CONTENT THAT MAY BE DAMAGING TO AMPNODE HOSTING'S SERVERS, OR ANY OTHER SERVER ON THE INTERNET."

Q. When someone creates an account with a booter service, do they have to ask the site administrator to conduct attacks for them?

A. No

Q. Is this because the attacks are automated?

A. Yes

Q. And the site administrator or owner, do they advertise that they want to illegally attack other websites?

A. No

4 – Show that booter services are a tool

Q. In fact, on both Downthem.org and Ampnode.org, they do state that the DDOS attack tools are for stress testing only and are not for illegal attacks, is that correct?

A. Yes

Q. In their testing, the FBI noted that they purchased a minimal account from Downthem.org, did you see that?

A. Yes

Q. And this account is what the FBI tested, correct?

A. Yes

Q. To the best of your knowledge, did the FBI ever purchase one of the higher bandwidth accounts for testing?

A. No

5 – Show that amplification server lists are a tool

Q. The amplification lists that the website sells. Do they advertise them for illegal use or for testing?

A. Testing.

Q. Can they be used for illegal DDOS attacks?

A. Yes

Q. Can they be used for any other purpose?

A. Yes

Q. So the lists themselves are not attack tools, correct?

A. Yes

6 – IP Blacklisting - Show that “victims” were protected from DDoS anyway

Q. Are you familiar with IP Blacklisting?

A. Yes

Q. Can you explain what IP Blacklisting is?

A. It is a function of network security devices like firewalls to automatically blacklist IP addresses with suspicious traffic.

Q. And is this a way to stop or mitigate a DDOS attack?

A. Yes

6 – Country Blocking– Show that “victims” were protected from DDoS anyway

Q. Are you familiar with country blocking?

A. Yes

Q. Can you explain what country blocking is?

A. It is a function of network security devices like firewalls that can be used to automatically block or ignore traffic from IP addresses from particular countries.

Q. And is this a way to stop or mitigate a DDOS attack?

A. Yes

7 – Show Common Knowledge – Protecting from DDoS = Cybersecurity 101

Q. In your role in network security, are you familiar with ways to protect a website from DDOS attacks?

A. Yes

Q. Are these protection methods secret?

A. No

Q. So other network security engineers could find and implement these measures to prevent or mitigate DDOS attacks?

A. Yes

Outcome

- Defendant convicted facing up to 35 years
  - Sentencing mitigation – Show that no damage was actually done to anyone directly by the defendant.
  - Preserve for Appeal – No actual damage done – website was simply a tool that could be used for “white hat” testing.
    - No victims reported damage from either of the services operated by the defendant.

ENVISTA FORENSICS

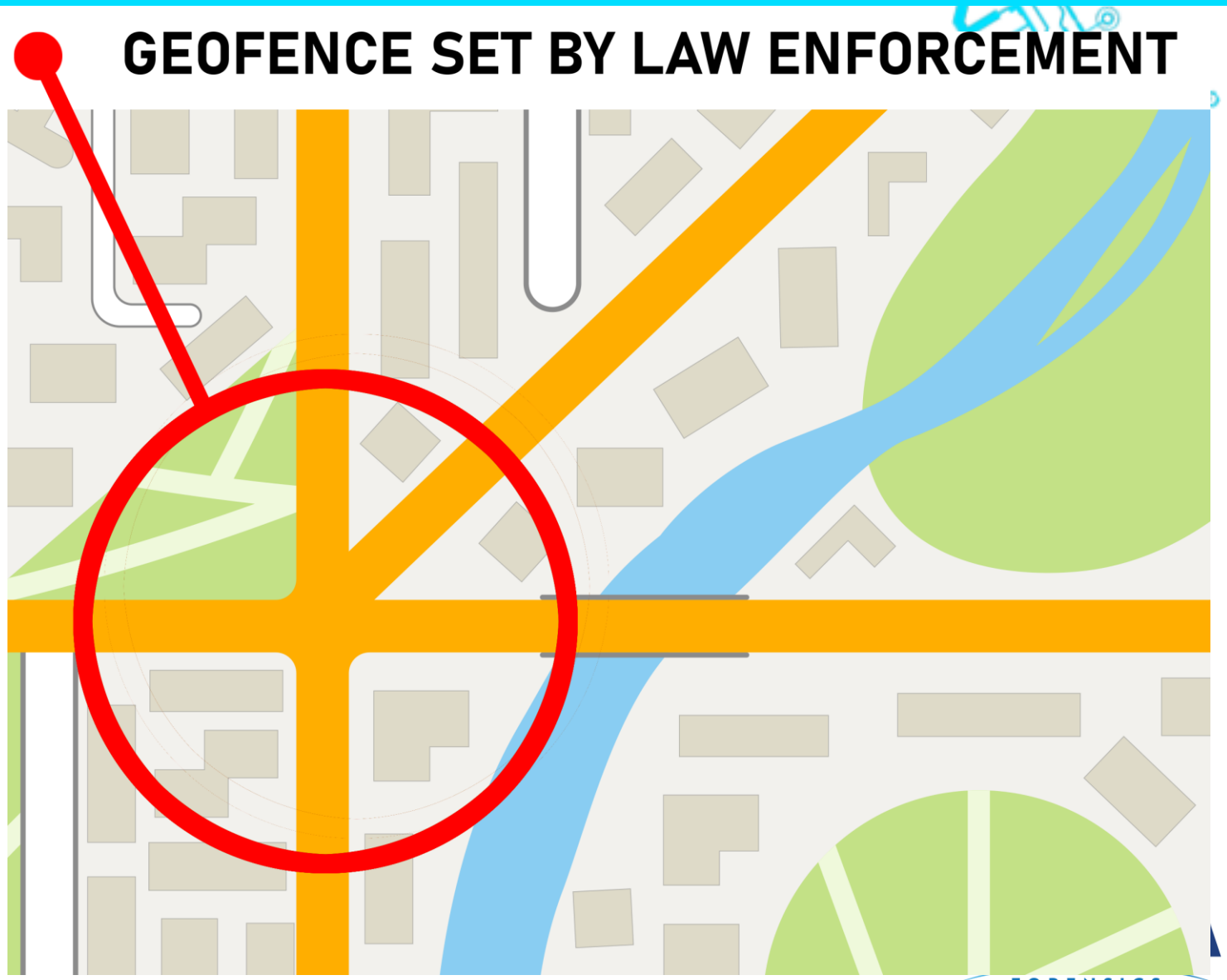
GOOGLE LOCATION SERVICES

CROSS EXAMINATION EXAMPLE

DIGITAL FORENSICS //

Location Data: Google GeoFence (GeoFence Warrant)

- GeoFence Warrant



Location Data: Google GeoFence (GeoFence Warrant)

1. LAW ENFORCEMENT DETERMINES THE COVERAGE AND TIMEFRAME OF INTEREST FOR THE GEOFENCE

2. EVERY SINGLE GOOGLE ACCOUNT WITH LOCATION HISTORY IN THE WORLD IS SEARCHED

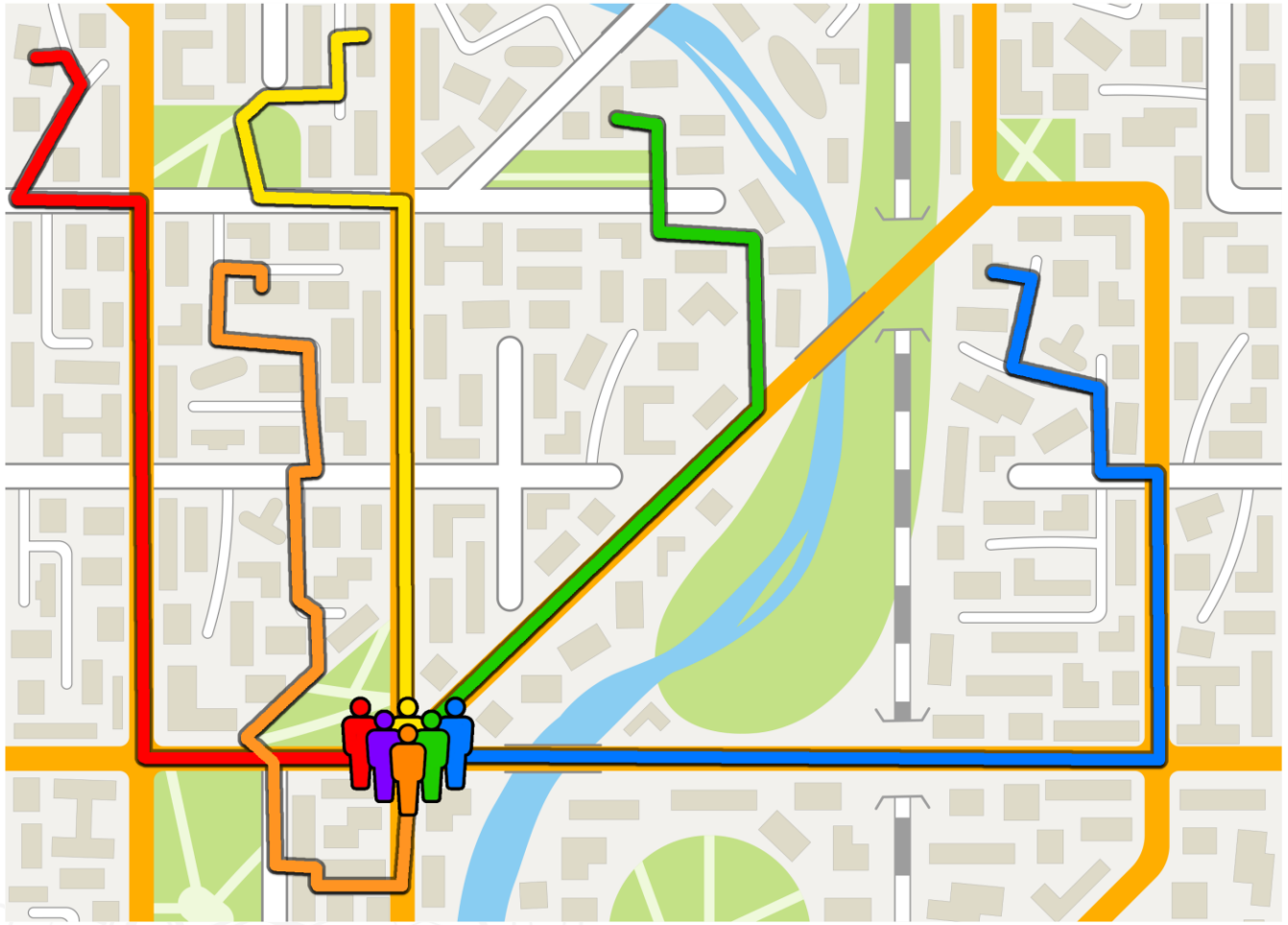
3. GEOFENCE IS POPULATED WITH EVERY PERSON IN THE AREA FOR THE DESIGNATED PERIOD

4. LAW ENFORCEMENT SELECTS SUSPECTS. THEY CAN NOW SEE THEIR ACTIVITY WITH NO GEOGRAPHIC LIMITS. (STEP 2)

ENVISTA FORENSICS

Location Data: Google GeoFence (GeoFence Warrant)

GEOFENCE IS REMOVED, ALL LOCATON ACTIVITY CAN NOW BE SEEN FOR THOSE PEOPLE LAW ENFORCEMENT HAS SELECTED



Location Data: Google GeoFence (GeoFence Warrant)

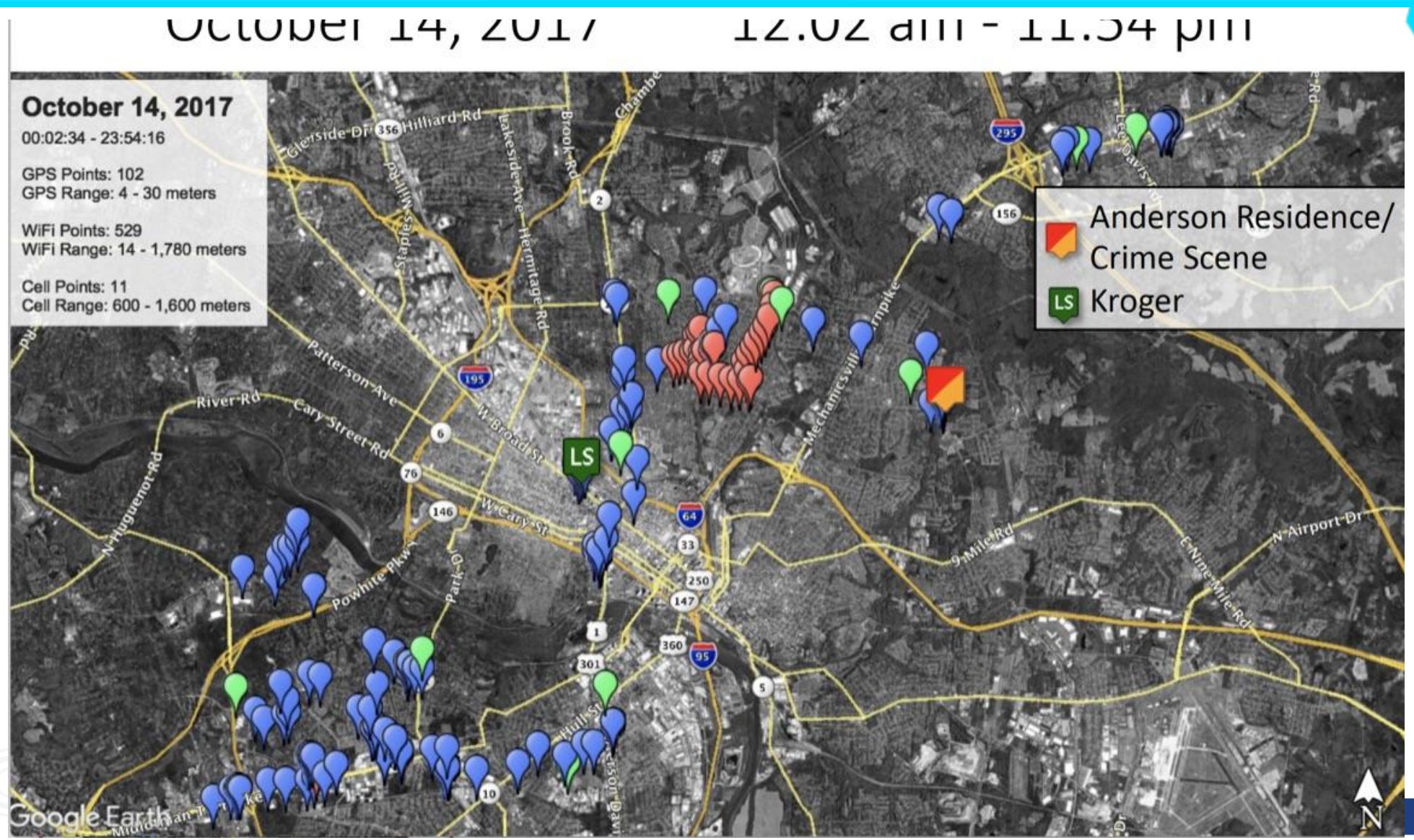
1. LAW ENFORCEMENT REQUESTS THAT GOOGLE REVEAL THE SUBSCRIBER INFORMATON OF SELECTED STEP 2 PERSONS OF INTEREST

2. GOOGLE PROVIDES THE SUBSCRIBER INFORMATION FOR THOSE LAW ENFORCEMENT HAS DESIGNATED AS PERSONS OF INTEREST

3. SUBSCRIBER INFORMATON INCLUDES THE USER'S ACCOUNT, EMAIL, PHONE NUMBERS, INTERNET PROTOCOL LOGS, AND OTHER DATA

ENVISTA FORENSICS

Location Data: Google GeoFence (GeoFence Warrant)



Direct Exam – Analysis and Plotting of Records

- Google Location Services
  - Sources: Records released by Google from Court Order or Search Warrant
  - Defense theory – location data was inaccurate (highly improbable, if not impossible)
- Objective
  - Limit Evidence (Daubert/Frye)
  - Limit Testimony
  - Preserve for Appeal
  - SEE ALSO: NACDL.ORG
    US VS. CHATRIE E.D. VA 3:19-CR-130

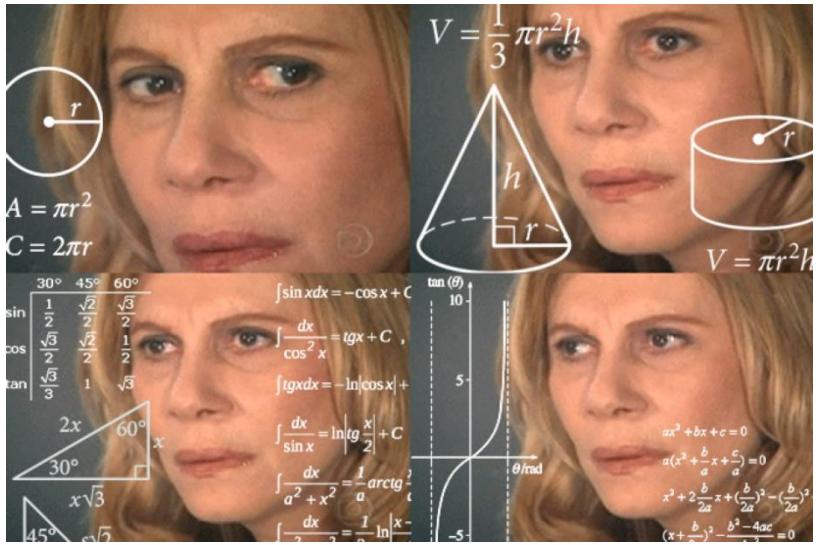
HENRICO COUNTY

Jury finds Henrico man not guilty of killing neighbor in 2017

Roland Anderson sentenced to 6 years after being found guilty of robbery

Direct Exam – Analysis and Plotting of Records

- Google Location Services
  - ownersEMAILaddress.LocationHistory.Records_001.zip
  - “Google Confidential & Proprietary”
  - “The Maps Display Radius field reflects an **estimated uncertainty** value regarding the reported coordinate. Its value depends on a great many factors and is an **approximation** sufficient for its intended product use



Direct Exam – Analysis and Plotting of Records

Q: Between 9:54PM and 10:36PM, you note several connections and recorded locations.

A. Yes

Q: What are the sources of these connections?

A. GPS, Cell and Wifi

Q: Regarding the GPS connections, they show between 16 and 48 meters. Are these within scientific standards?

A. Yes (well within reason)

Q: Regarding the "CELL" records, these vary between 1700 and 2400 meters, are these within scientific standards?

A. Yes

Q: Finally, regarding the "WIFI" connections, these vary between 30, 32, 34, 760, and 3,894 meters. (approx. 99, 104, 111, 2,500, 12,775 feet)

A. No; Consumer level WIFI 2.4GHz and 5GHz do not effectively transmit beyond 100 meters or 328 feet.

Display Radius (Meters)	Source
16	GPS
32	WIFI
32	WIFI
2400	CELL
2400	CELL
2400	CELL
2400	CELL
1700	CELL
1700	CELL
1700	CELL
30	WIFI
30	WIFI
2400	CELL
2400	CELL
760	WIFI
760	WIFI
3894	WIFI
3894	WIFI
3894	WIFI
34	WIFI

Direct Exam – Analysis and Plotting of Records

Q: If the theoretical limit of consumer Wi-FI (2.4-5GHz), when amplified, is 250 meters (820 Feet), how do you explain the records of 760 and 3,894 meters?

A. These are anomalies. We do not know.

Q: How does Google collected these records?

A. Via applications within the Android Operating System and in devices running Google applications.

Q: And since you do not work for Google, you cannot tell us what the intended purpose of these records is, correct?

A. I cannot.

Range comparison – 2.4 GHz vs. 5 GHz signal

Frequency	Theoretical Distance	Real-World Distance
2.4 GHz (802.11b)	460 ft	230 ft
2.4 GHz (802.11g)	125 ft	62 ft
2.4 GHz (802.11n)	820 ft	410 ft
5 GHz (802.11a)	390 ft	195 ft
5 GHz (802.11ac)	up to 820 ft (amplified)	up to 410 ft (amplified)
5 GHz (802.11n)	460 ft	230 ft

ENVISTA FORENSICS

CELLULAR LOCATION

CROSS EXAMINATION EXAMPLE

DIGITAL FORENSICS //

Cellular Location – Sample Voir Dire

Q. Can you tell the court what CDMA is?

A. CDMA stands for code division multiple access.

Q. Can you explain how CDMA works?

A. CDMA is a channel sharing technology where all of the cell phones in an area of coverage use the same radio frequency. The different conversations have a unique code. An easy way to think of CDMA is as if you had several couples in a room. Each couple speaks a different language. Imagine that couple one is speaking English while couple two is speaking Japanese. Since they don't understand the other languages, those other couple's conversations are just noise to them.

Q. And can you tell me what GSM stands for.

A. GSM stands for Global System for Mobile Communications.

Q. Can you tell the court which wireless telephone companies use GSM?

A. AT&T and T-Mobile use GSM in the united states.

Cellular Location – Sample Voir Dire

Q. And how about CDMA.

A. CDMA is basically all the other companies: Verizon, Sprint, US Cellular, Metro PCS

Q. Can you tell me what GPRS stands for?

A. General Packet Radio Service.

Q. Can you tell me what PSTN stands for?

A. PSTN stands for the public switched telephone network. This is the wired landline telephone network.

Q. Can you tell us what the two dominant radio frequencies used the cellular telephone network?

A. 850 MHz and 1900 MHz (megahertz)

Q. Can you explain what free space loss is?

A. Free space loss or attenuation is the way that radio waves fade over distance.

Q. Can you tell me what Rayleigh fading is?

A. Rayleigh fading or multi-pathing is the way a radio signal fades or weakens when the signal is bounced off several objects. This breaks the signal in to multiple pieces and the cell phone puts them back together.

Cellular Location – Sample Voir Dire

Q. Can you explain what radio propagation is?

A. Radio propagation is how the radio waves expand outward from the cell tower.

Q. Can you explain what the dominant area of a cell tower's coverage is?

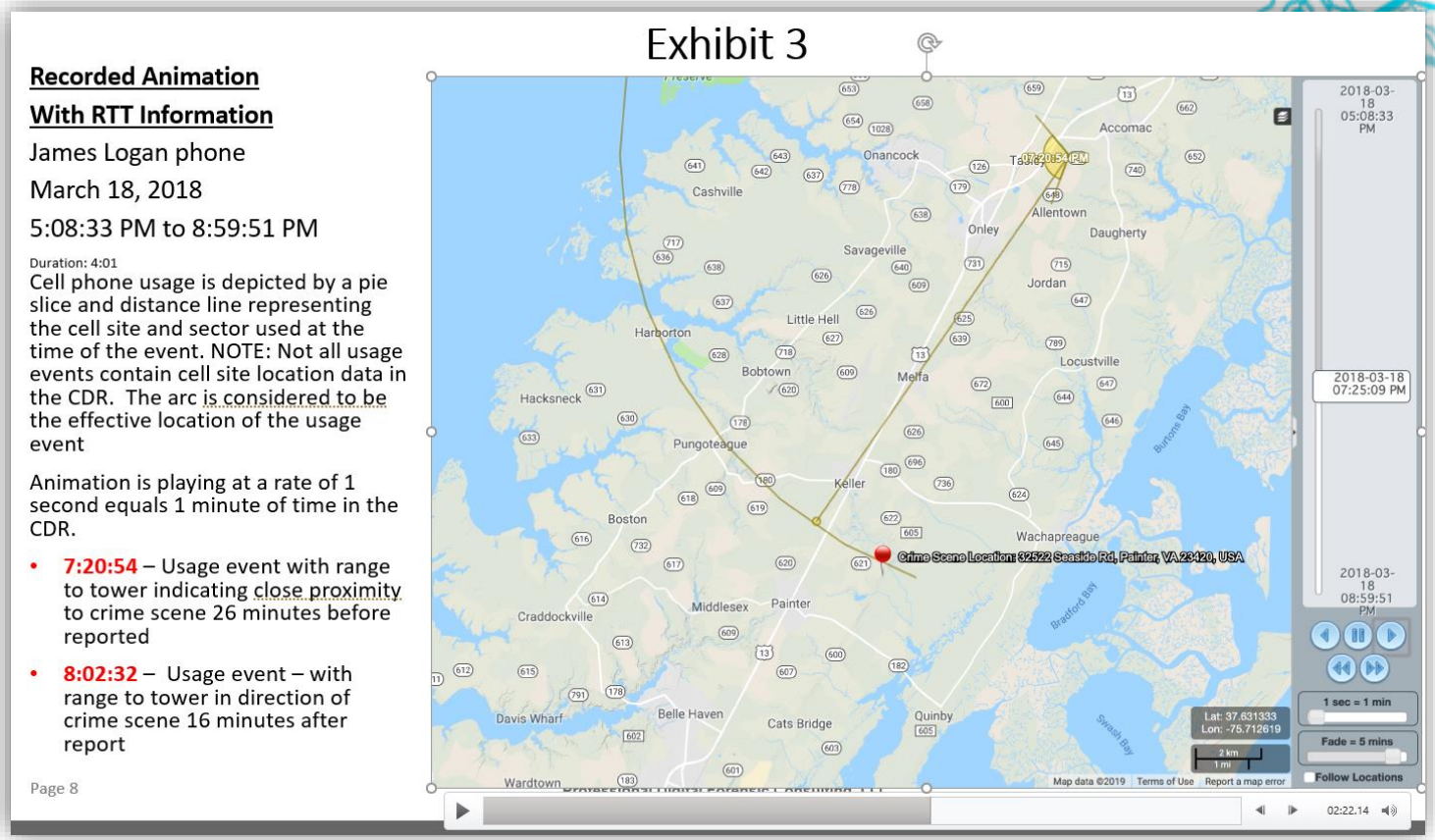
A. It is the area near the tower where the signal is so strong a phone cannot choose a different tower.

Q. Can you explain what a neighbor list is?

A. In the GSM system, the phone is provided with the towers that surround the phone by the network. The phone then stacks the towers in order of best signal. It uses this to choose the tower that is will using to connect a call.

RTT (Real Time Tool) Records – Verizon Wireless

- Opposing expert attempting to use RTT to place defendant at the scene
  - Estimated Latitude/Longitude reported by Verizon was not accurate, and he attempted to explain away these issues in his report. However, he could not hide these issues from a solid cross exam



1 – Difference between CDR and RTT

Q. So you indicated that a tower and sector can be used to determine the location of a device correct?

A. Yes

Q. And these RTT records go a step further and provide an estimated latitude and longitude for the device and an estimated distance from the tower and sector as well, correct?

A. Yes

Q. And you can generally locate the device with just a tower and sector can't you?

A. Yes

Q. Isn't it true that the phone determines the tower and then the sector that best provides service to complete a call or other transmission?

A. Yes

Q. And it uses the sector that is providing the best coverage at that moment correct?

A. Yes

Q. It does not use two sectors at the exact same moment does it?

A. No

1 – Difference between CDR and RTT

Q. So looking at your page marked exhibit 43, go to about 15-16 seconds on that slide. You see the transaction at 5:19 PM correct?

A. Yes

Q. The sector faces the area of Daugherty, correct?

A. Yes

Q. Point and show us the sector and indicate to the jury which way that sector would project the signal.

A. (towards the coast, Daugherty area)

Q. and that yellow arc is the estimated distance, correct?

A. Yes

Q. Indicate that to the jury too please.

A. (points)

Q. Now point to the estimated latitude and longitude made by Verizon.

A. (north of Greenbush)

2 – Show contradiction – two sectors (places) at once

Q. The area covered by the arc is quite some distance from the estimated lat/lon isn't it?

A. Yes

Q. This tower, sector, estimated distance and estimated pinpoint are all from one row in the record isn't it?

A. Yes

Q. This calculation is made by Verizon at one exact moment isn't it?

A. Yes

Q. You cannot be in Greenbush and south of Jordan at the same time can you?

A. No

Q. please use the scale at the bottom of your map and tell us how many miles it is from the pinpoint to the arc between Jordan and Locustville.

A. about 7 miles

Q. Which is the accurate location, North of Greenbush or South of Jordan?

A. ????

2 – Show contradiction – two sectors (places) at once

Q. Point of the map to the exact physical location of the device at 5:19 PM?

A. he cannot

Q. (point near the dot at Greenbush) Can the phone be here?

A. possibly

Q. (point anywhere along the arc) can it be here?

A. possibly

Q. These are two completely separate sectors of coverage aren't they?

A. yes

Q. And you cannot be at two places at once can you?

A. No

3 – Expose the misleading and flawed analysis

Q. So again, the phone can be located any where along the arc right?

A. Yes

Q. So the phone could be in Keller?

A. Yes

Q. And the phone could be in Pungoteague?

A. Yes

Q. It could also be at the dot couldn't it?

A. Yes

Q. How many miles is the dot from the incident location?

A. About 3 miles

3 – Expose the misleading and flawed analysis

Q. and you say as a result of 3 miles that this mean in “close proximity”?

A. Yes

Q. The width of the peninsula is only about 9 miles or so correct?

A. Yes

Q. So 3 miles is in close proximity to nearly everything on the peninsula, right?

A. Yes (even the arc is about a mile away, so still not that close)

4 – Expose the truth – misleading reporting and contradictions

Q. Point to the map to show the jury the exact location of the phone at this time please.

A. He cannot

Q. so at no point during this presentation can you point to the map and show us the location of the device?

A. No

Q. And in some of the information you have here, the records contradict themselves placing the phone in two locations at once?

A. Yes (show him exhibit 43, at 16 seconds, if he does not agree)

4 – Expose the truth – misleading reporting and contradictions

Q. Point to the map to show the jury the exact location of the phone at this time please.

A. He cannot

Q. so at no point during this presentation can you point to the map and show us the location of the device?

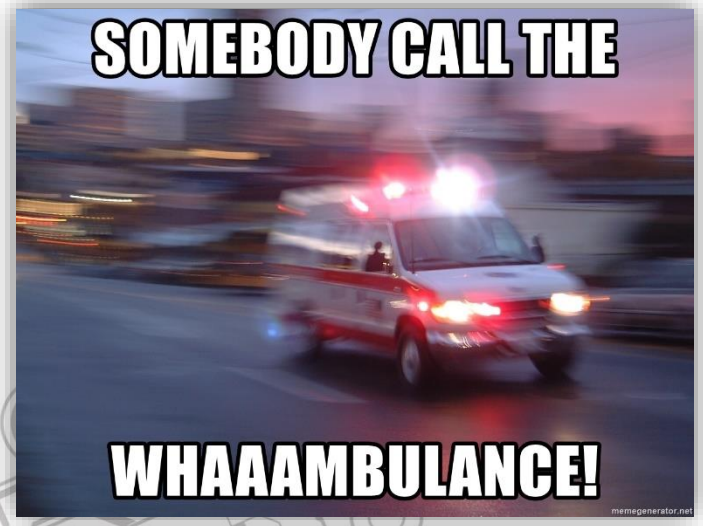
A. No

Q. And in some of the information you have here, the records contradict themselves placing the phone in two locations at once?

A. Yes (show him exhibit 43, at 16 seconds, if he does not agree)

Outcome

- Some “experts” will say whatever their client wants them to say. Regardless of integrity. I recently had an “expert” from Envista Forensics state no less than 8 times in his report that I was deceiving, obfuscating, and misleading the jury with my findings, essentially repeatedly calling me a liar with no foundation.
  - Nowhere in our expert’s report are the words deceiving, obfuscating, or liar used.



ENVISTA FORENSICS

CASE EXAMPLES

ANALYSIS AND REPORTING

DIGITAL FORENSICS //

Preparing your Attorney

- Aaron Hernandez case
  - Patriots Football player accused of murder

Preparing your Attorney

- Casey Anthony
  - "Forensic Fantasy"

Case Examples - Pheedo

- Challenging the Evidence
  - User inputted search terms?
    - Listed below are the notable keyword searches and number of "hits" that FTK noted

- "Homicide" 230 hits
- "Homicidal" 540 hits
- "Insanity" 178 hits
- "Defense" 2429 hits
- "Defense and Insanity" 871 hits
- "Wikipedia" 6034 hits
- "Murder" 2497 hits
- "Deathblow" 16 hits
- "Pheedo" 155903 hits
- "Kill" 9010 hits
- "Police" 5788 hits
- "Killer666vampire" 4863 hits
- "Killer" 3872 hits
- "Insane" 4308 hits
- "Death" 7745 hits
- "BTK" 1174 hits

Case Example – Pheedo

- Challenging the Evidence
  - User inputted search terms?

“Detective noted that the user inputted a search term or key word of "homicide". In addition the user inputted key words of "Attorney General" and also "Preterm Birth" The date on this particular example is dated August 5, 2010”

href="http://ads.pheedo.com/click.phdo?s=126e398be33ab04abbf5858c463a8ac1&p=64&kw=Hidalgo">Hidalgo - <a

href="http://ads.pheedo.com/click.phdo?s=126e398be33ab04abbf5858c463a8ac1&p=64&kw=Homicide">Homicide - <a

Case Example – Pheedo

- Challenging the Evidence
  - User inputted search terms?

Case Example - Pheedo

- Challenging the Evidence
  - User inputted search terms?

\Desktop\C\i386\Apps\App000102\common\msshared\wkshared**msgr3en.lex**
insatiably $J £ J Ìþ insatiable = = ¡ 1 insanity $J ¡ J Ìþ insanitary ! d ` 2 insanely $Jÿ
12/16/06 02:15:19PM 12/16/06 02:15:19PM 03/09/05 07:11:46PM

\Desktop\D\Recovered Folders**pptico.exe**
see me wrestle this Saturday afternoon :) A Fair Amount Of Insanity â€Ž"A FAIR AMOUNT OF INSANITY" is an annual wrestling event

11/30/06 05:47:01PM 11/30/06 05:47:01PM 11/30/06 05:47:01PM
\Desktop\D\Recovered Folders**pptico.exe**
afternoon :) A Fair Amount Of Insanity â€Ž"A FAIR AMOUNT OF INSANITY" is an annual wrestling event put on by

11/30/06 05:47:01PM 11/30/06 05:47:01PM 11/30/06 05:47:01PM
\Desktop\D\Recovered Folders\.\Windows\SoftwareDistribution\DataStore**DataStore.edb**
tely wasn't int s jeffdunham 0:39+ Jeff Dunham: spark of insanity bed scene, walte... 1,833,051 views
hoppajinxy 7:17+ 12/16/06 02:37:14PM 12/16/06 02:37:14PM 08/08/10 01:42:15AM

Case Example – Time Games

- Boston Case
  - Possession, Distribution, Receipt of Child Porn
    - Yahoo Messenger Chat
      - Roleplay is real.
    - Adult vs. Child Porn
      - Amount and source matter.

Case Example – Time Games

- Boston Case
  - Tens of thousands of adult porn files and only a few child porn files.
    - In this case, search terms unrecoverable

Like "*sex*" Or Like "*porn*" Or Like "*pussy*" Or Like "*suck*" Or Like "*hor*" Or Like "*dick*" Or Like "*nude*" Or Like "*tranny*" Or Like "*shemale*" Or Like "*ass*" Or Like "*rape*" Or Like "*fuck*" Or Like "*teen*" Or Like "*lesb*" Or Like "*cock*" Or Like "*anal*" Or Like "*incest*" Or Like "*cum*" Or Like "*girl*" Or Like "*tit*" Or Like "*BDSM*"

The following are the 10 files that were not located using the adult search terms:

From the Saved Folder

Number	Limewire Saved_File Exam For Content.Name
1	Jerry Springer - uncut.avi
2	We Live Together - Lexi (full).mpg
3	Pedo (Pthc) - Little 6yo and dad (Hussyfan) (r@ygold) (babyshivid) - sound, heavy crackling.mpg
4	Jerry Springer Too Hot For Tv 5.mpg
5	Jerry Springer - I Refuse To Wear Clothes 5.mpg
6	eva mendas.mp3
7	Da Ali G Show - Borat Tries To Buy A Slave.mpg

Case Example – Time Games

- Boston Case
  - Tens of thousands of adult porn files and only a few child porn files.
    - Law enforcement later determined all chat partners were adults

Further, a screenname such as "judy12_needdaddy" (File 1 in "IM's Of Interest from [redacted] report) no more informs someone that Judy is 12 years old than "cute_molly81" informs someone that cute_molly is 81 years old. Numbers in a screenname can mean something, or they can be entirely meaningless. Even if the numbers do have some sort of meaning, it does not necessarily mean that another person would know the significance behind the numbers.

Due to the anonymity of the internet, it is common knowledge in the forensics community that chat rooms, and in particular sexually oriented chat rooms, are commonly used by persons for the purpose of roleplay. This roleplaying can come in the form of various sexual fetishes, and given Yahoo's policies concerning the age restriction of 18 years or older to access Yahoo Messenger chat services, someone claiming to be underage could be determined to be of age and roleplaying by a user of Yahoo Messenger when chatting with that person.

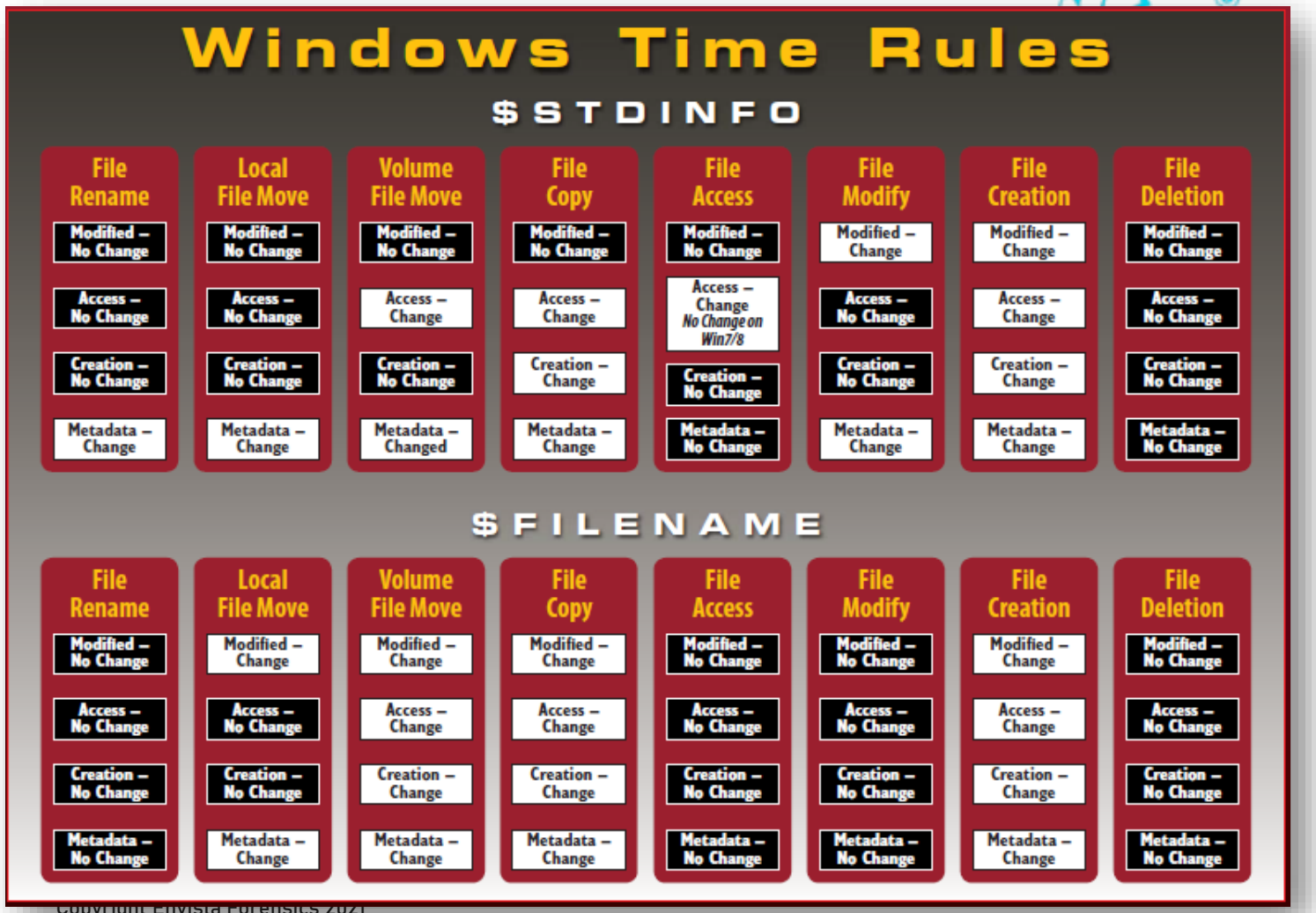
Case Example – Time Games

- Boston Case
  - Download times match chat records?
    - Affidavit about computer times
    - Law enforcement examiner could not testify as expert

Case Example – Time Games

- Fact Witness vs. Expert Witness
  - Affidavit about computer times
  - Law enforcement examiner could not testify as expert

- SANS Forensics Windows Forensic Analysis Poster, www.sans.org



Expert Testimony

- Boston Case
  - Download times match chat records?
    - Affidavit about computer times
    - Law enforcement examiner could not testify as expert

18. The basis for Detective [redacted] "looking at times that the videos were created and looking at other items that occurred around that time" is also based upon a basic misunderstanding of the computer file system and how the peer to peer file sharing software Limewire works. The created date of the video file *does not* relate to user activity. The created date of the video file would indicate the time the file *finished* downloading. The date the file finishes downloading can be hours or even days after any actual user activity took place. This renders the examination of Limewire video created dates to "other items that occurred around that time" nonsensical.

ENVISTA FORENSICS

DIGITAL FORENSICS IS DIFFERENT

INFORMATION TECHNOLOGY IS NOT DIGITAL FORENSICS

DIGITAL FORENSICS //

Selecting an Expert: Overview

- Actual training in digital forensics?
  - IT training is not forensic training
- Digital forensics certifications?
  - IT certifications are not forensics certifications
- Actual case experience?
  - Experience in the type of case you have?
- Recommended by other professionals?
  - In particular other attorneys

Why A Forensic Expert?

- Digital Forensic Expert
  - Should have comparable or better training that other expert
  - Specific training and experience in digital forensics
  - Should have access to same or better tools than other expert
  - Must be able to qualify as a forensic expert in court

Forensic Tools

- True barrier to entry – COST
  - Do they have the appropriate tools?
    - Necessary in today's world
      - Too many forensic artifacts
    - Required to perform many digital forensics functions
    - Almost always needed to perform forensically sound acquisitions and examinations

Expectations of a Forensic Expert

- Digital Forensic Expert
  - Expected To:
    - Anticipate testimony of opposing expert based on:
      - Forensic reports, discovery
    - Duplicate and verify opposing expert's work
    - Assist the attorney in preparation for trial
      - Consultation
      - Direct examination
      - Cross examination
    - Advise attorney as to the merits of the case regarding the digital evidence
      - Assist attorney in explaining merits or potential issues with their case based upon forensic evidence

Expectations of a Forensic Expert

- Digital Forensics Expert
  - Expected to testify if needed as to:
    - Various files on the client's device
    - Ownership of the devices and files
    - Forensic processes used in the extraction and analysis
    - Handling and collection of the evidence
    - Specifics related to dates and times

Case Example – Wrong Expert

- RALEIGH (WTVD) - The defense asked for a mistrial Tuesday in the Brad Cooper murder trial.
- The move came as the first witness for the defense endured a withering examination by the prosecution on his qualifications to testify as an expert.
- James Ward of WireGhost Security told the court he was an expert in computer network security, but the prosecution questioned his qualifications to testify about Cooper's computers as a forensics expert.

Case Example – Wrong Expert

- Arguing before Gessner Tuesday, the prosecution said Ward lacked the proper education and experience to say there was evidence of computer tampering.
- "He has a home lab. He borrowed his tools from Cisco. He doesn't know what software he used," said prosecutor Boz Zellinger.
- Zellinger said the prosecution and defense should be held to the same standards on expert witnesses, and Ward falls short.
- "I would be laughed out of this building," said Zellinger.
- Gessner ruled that Ward could testify about network security, but he could not testify about the FBI reports on Cooper's computers.

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - Multiple User Access

Conclusion #1: Multiple users inside and outside the household accessed the Gardner family computer.

Moshlak presumes there were multiple users of the computer . . . based on the existence of computer directories and files bearing different names and containing resumés of individuals other than Gardner. Even though the United States agrees that several members of the Gardner family had access to the computer . . ., the court will not allow Moshlak to testify about his conclusion as it is presently worded. As written, his conclusion is not an expert conclusion based on scientific, technical, or other specialized knowledge.

Whether more than one person, and, if so, who, used the computer, is a fact question for the jury to decide. Moshlak's proffered testimony would usurp the role of the jury. Moshlak, however, will be allowed to testify that during his review of the Gardner family computer, he observed files, directories, and documents with names other than Bryan Gardner. He may not extrapolate further.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - Generic computer user account

Conclusion #2: "HP Owner" was the generic user name assigned to anyone accessing the family computer

This conclusion is relevant. But the court is concerned with the phrasing used by Moshlak. The court will allow Moshlak to state his opinion, but only if it is framed in a way that more accurately reflects the nature of the fact (and to the extent it is not cumulative). That is, rather than stating that the `HP_Owner' was not associated with Gardner, Moshlak may point out that the `HP_Owner' name was not associated with or assigned to any particular individual using the computer.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - No RIDs and SIDs (Particular User Accounts)

Conclusion #3: No Relative Identifiers (RIDs) or Security Identification Descriptors (SIDs) were associated with Gardner on the family computer

The analysis of Conclusion 2 also applies here. The court finds the lack of RIDs and SIDs to be somewhat relevant. However, Moshlak may not present his opinion in the matter phrased in his report. He may point out to the jury that there are no RIDs or SIDs associated with anyone on the Gardner family computer. This is more accurate than the artificial spin he places on the lack of RIDs and SIDs in an effort to eliminate Gardner as a possible user of the family computer.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - Computer forensics experts as investigators?

Conclusion #5: The [Regional Computer Forensic Laboratory] report did not identify any actors and so the report, as well as the analysis of Government agents who generated the report, is insufficient.

The court agrees with the United States that this conclusion is not relevant, not based on scientific, technical or other specialized knowledge, and is not based on sufficient facts or data. The RCFL computer forensics examiners do not do investigative work. Moshlak's conclusion assumes they are required to do so in order to do their jobs effectively. But the type of investigation to which Moshlak is referring was not part of the RCFL experts' scope of work.

Moreover, Moshlak has no specialized expertise regarding the job of a government computer forensic examiner. As the United States notes, the Department of Justice guide for law enforcement is not sufficient data for Moshlak to speculate about what individuals involved with this case should have done. The court excludes any testimony of this nature.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - Thumbs.db Dates

Conclusion #6(B): The image modification dates in the thumbs.db file suggest that Gardner could not have downloaded or viewed the images because the dates coincide with the dates Mr. Gardner was in prison.

Based on a long colloquy during the Daubert hearing, Moshlak admitted that the modification dates in the thumbs.db file do not have any bearing on whether Gardner downloaded or viewed the images on the Gardner family computer. . . .Accordingly, this conclusion is excluded as unhelpful to the jury.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - Yahoo Companion toolbar

Conclusion #9: Yahoo Companion toolbar has a button for kidpower12345@yahoo.com that allows anyone to access the email account.

The United States contends that although `[t]he fact that kidpower12345 is in Yahoo Companion is not disputed, the conclusion about how it works is not based on sufficient facts or reliable methodologies. . . .The court agrees.

As part of his conclusion, Moshlak testified that `anybody that goes ahead and activates a Web browser has the ability to go ahead and log in as kidpower12345[.]' . . . Moshlak provided no factual basis for such a conclusion or any reason for the court to believe that he has expertise regarding the Yahoo Companion toolbar or that he can explain why he reached this conclusion.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - Traceroute

In his report, Mr. Moshlak states,

No traceroute data analysis was provided, as to the network which was used, in determining if a nexus between [Gardner] and his USB modem could be established. In review of the material provided [sic] shows no Verizon Access Manager connectivity, but does show QWEST as a potential provider of services. In addition an IP address analysis was performed based upon the Username logons and user names provided [by] Ning, and the IP address data that was provided in this case, with the user logon, related to a number of different areas in the nation. A number of these IP addresses resolved to various other parts of the nation, including [over twenty locations within the United States]. . . .

On the stand, Moshlak himself admitted that he did not know how someone could log-in over 300 times on a particular date or from multiple locations throughout the country. He said, `something tells me something isn't right. We ought to go back and take a look at it.' Unless and until the defense can come up with a more thorough analysis and explanation for the conclusion, Moshlak's testimony in this area is excluded.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - Viruses!

Conclusion #13: There were viruses on the Gardner family computer.

During testimony, Moshlak admitted under cross-examination that the viruses could not have created the images of child pornography in the thumbs.db folder. Absent any evidence (other than the speculation offered by [Gardner]) that a third party hacked into the Gardner family computer to download the offending images, Moshlak's conclusion is, at best, not relevant, and would confuse the jury.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

Spotting a Problem Expert

- Example:
  - United States v, Bryan James Gardner
    - Child Porn Case – Daubert Hearing

The judge therefore granted the prosecution's motion to exclude Moshlak's expert testimony in part and denied it in part.

http://cyb3rcrim3.blogspot.com/2013/01/child-pornography-expert-witness-and.html

ENVISTA FORENSICS

ASK YOUR EXPERT FOR INTEL

EVEN IF YOU DON'T NEED AN EXPERT CALL AND ASK ABOUT THE OPPOSING EXPERT

DIGITAL FORENSICS //

Spotting a Problem Expert

- Example – Engineer or not..?

Education

Year	College or University	Degree
1981	University of Connecticut	Electrical Engineering (coursework only)

Spotting a Problem Expert

- Example – Engineer or not..?

Q. And you kind of shared with us a moment ago, but do you consider yourself an expert in any particular fields?

A. Yeah. I'm an expert in telecommunications specifically. I'm an electric engineer and my job has been to have expertise in cell phones, in mobile communication. The -- I've been involved for 30 years

Spotting a Problem Expert

- Example – Engineer…you decide.

You Can Officially Call Yourself an Engineer Only If You Have a PE License

If you do not have a PE license, you cannot officially call yourself an engineer -- and your company cannot identify you as an engineer -- in official documents, such as business cards, letterheads and resumes. Additionally, you will need to register as a PE if you decide to work for yourself as a consultant.

https://www.monster.com/career-advice/article/professional-engineer-license-pe

Questions?

lars.daniel@envistaforensics.com / 919-621-9335
Jake.green@envistaforensics,com / 984-269-2709